CLAIMS

1. An anti-virus file scanning system for computer files comprising:

a) a computer database containing records of known executable programs which are deemed to be not malware and criteria by which a file being processed can be determined to be an instance of one of those programs;

b) means for processing a file being transferred between computers to determine whether the file matches the criteria characterising a file as an unchanged instance of a program in the database; and

c) means for signalling the file as known or not depending on the determination made by the processing means.

2. A system according to claim 1 and including:

d) means for processing an inputted file to determine whether it is considered to be, or considered possibly to be, infected with a virus, and wherein, in operation of the system, a file is subjected to processing by the means d) unless the file is signalled as safe by the signalling means c).

3. A system according to claim 1 or 2 wherein the processing means b) comprises

b1) a file recogniser for determining whether the file being processed is an instance of a known file and

b2) a difference checker for checking whether the file is an unchanged version of that known file.

4. A system according to claim 3 wherein the file recogniser includes means for checking the contents of the file being processed for the presence of at least one characteristic signature associated with a file which is considered to be known and uninfected.

5. A system according to any one of the preceding claims wherein the processing means b) includes means for generating a checksum for the entire file under

consideration or for at least one selected region thereof, and means for comparing the checksum or checksums with those of entries in the database.

6. A system according to any one of the preceding claims and including an exception list handler for determining, in relation to a file which the processing means b) has determined is not a known file, whether that file has characteristics matching an entry in an exception list of files, and the signalling means is operative to signal the file as malware if it is not in the exception list or as unknown if it is.

7. A method of anti-virus scanning system computer files comprising:

maintaining a computer database containing records of known executable programs which are deemed to be uninfected and criteria by which a file being processed can be determined to be an instance of one of those programs;

processing a file being transferred between computers to determine whether the file matches the criteria characterising a file as an unchanged instance of a program in the database; and

signalling the file as known or not depending on the determination made by the processing means.

8. A method according to claim 7 and including:

processing an inputted file to determine whether it is considered to be, or considered possibly to be, infected with a virus, and wherein, in operation of the system, a file is subjected to processing by the step d) unless the file is signalled as safe by the signalling step c).

9. A method according to claim 7 or 8 wherein the processing step b) uses b1) a file recogniser for determining whether the file being processed is an instance of a known file and b2) a difference checker for checking whether the file is an unchanged version of that known file.

10. A method according to claim 9 wherein the file recogniser includes means for checking the contents of the file being processed for the presence of at least one

characteristic signature associated with a file which is considered to be known and uninfected.

11. A method according to any one of claims 7 to 10 wherein the processing step b) includes generating a checksum for the entire file under consideration or for at least one selected region thereof, and comparing the checksum or checksums with those of entries in the database.

12. A method according to any one claims 7 to 11 and including using an exception list to determine, in relation to a file which the processing step b) has determined is not a known file, whether that file has characteristics matching an entry in an exception list of files, and wherein, in the signalling steps, the file is signalled as malware if it is not in the exception list or as unknown if it is.